ISSN 2222-2944. Інформаційні технології: наука, техніка, технологія, освіта, здоров‘я. 2017. Ч. II

АНАЛИЗ ЭФФЕКТИВНОСТИ ПРИМЕНЕНИЯ МЕТОДА ПОСТРОЕНИЯ СИНДРОМНО ТЕСТИРУЕМЫХ СХЕМ К АППАРАТНЫМ РЕАЛИЗАЦИЯМ КРИПТОГРАФИЧЕСКИХ ПРЕОБРАЗОВАНИЙ

Караман Д.Г.
Национальный технический университет «Харьковский политехнический институт», г. Харьков

Метод синдромного тестирования заключается в приложении к проверяемой схеме полного тривиального исчерпывающего теста и подсчете числа единиц (нулей), которые появляются на наблюдаемом выходе схемы, как реакция на приложение последовательности тестовых наборов.

Достоинствами метода является простота реализации диагностического эксперимента, в ходе которого используются двоичные счетчики и схемы сравнения, а также исключение дорогостоящей процедуры машинного синтеза проверяющих тестов. Однако платой за простоту процедуры диагностирования является либо невысокая достоверность результатов диагностирования для произвольной комбинационной схемы (КС), либо необходимость применения специальных методов анализа КС и ее последующей модификации, для обеспечения покрытия обусловленного класса неисправностей.

Криптографические преобразования являются очень чувствительными к ошибкам, возникающим в процессе их выполнения. Вследствие высокой нелинейности этих преобразований, их дистрибутивности и итеративности процесса шифрования даже одиночные битовые ошибки быстро распространяются на весь массив обрабатываемых данных, приводя в негодность итоговый результат без какой-либо возможности восстановления.

Метод синдромного тестирования хорошо подходит для организации диагностической инфраструктуры отдельного класса криптографических преобразований, выполняющих процедуру нелинейной подстановки отдельных блоков исходных данных. Из-за больших массивов обрабатываемых данных и нелинейного характера преобразований, часто не имеющего какого-либо функционального описания (преобразования выполняются по специальной таблице-словарю) подстановочные модули являются наиболее сложными объектами для диагностирования одиночных константных неисправностей, приводящих к описанным выше ошибкам.

В докладе рассмотрен вопрос достоверности получаемых результатов диагностирования синдромно тестируемых подстановочных модулей в криптографических преобразованиях: рассмотрена обновленная модель неисправностей, которые могут возникать в конфигурируемых логических блоках и матрицах межсоединений современных ПЛИС-архитектур, представлены результаты экспериментов с подстановочными блоками различных блочных алгоритмов шифрования, сформулированы критерии оценки эффективности применения метода построения синдромно тестируемых схем к аппаратным реализациям криптографических преобразований.